(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 May 2001 (03.05.2001)

PCT

(10) International Publication Number
WO 01/31923 A1

(51) International Patent Classification[7]: H04N 7/167

(21) International Application Number: PCT/US00/41520

(22) International Filing Date: 24 October 2000 (24.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/427,776 26 October 1999 (26.10.1999) US

(71) Applicant: **MKPE CONSULTING** [US/US]; PMB 519, 23679 Calabasas Road, Calabasas, CA 91302 (US).

(72) Inventors: **KARAGOSIAN, Michael, A.**; 3981 Black Bird Way, Calabasas, CA 91302 (US). **MCKINNEY, Clyde, R.**; 208 Rutherford Drive, Danville, CA 94526 (US).

(74) Agents: **SMITH, Albert, C.** et al.; Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306 (US).

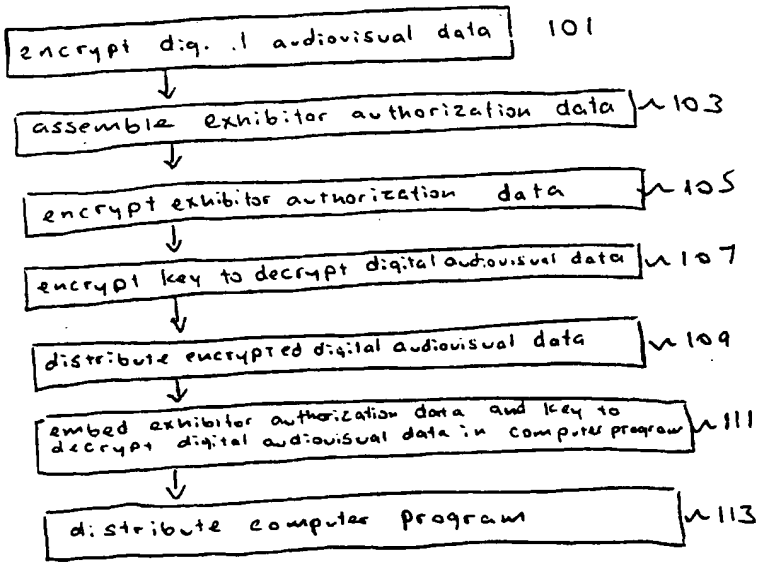
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR ENSURING SECURE DISTRIBUTION AND RECEIPT, AND SECURE AUTHORIZED EXHIBITION OF DIGITAL AUDIOVISUAL DATA



(57) Abstract: An exhibitor receives encrypted digital audiovisual data (103) and exhibitor authorization data from a distributor. Authorization of the exhibitor to exhibit the digital audiovisual data is ensured by comparing the exhibitor authorization data to exhibitor provided identification data. The audiovisual data is decrypted (107) and exhibited only upon verification of the exhibitor's authorization. The audiovisual data is watermarked with identifying information (111) so that pirated analog copies made from the exhibition can be traced to the source.

Method and Apparatus for Ensuring Secure Distribution and Receipt, and Secure Authorized Exhibition of Digital Audiovisual Data

Inventors: Michael Karagosian, Clyde McKinney

Field of the Invention

The present invention relates generally to secure data communication, and more specifically to secure distribution, receipt, and exhibition of digital audiovisual data.

Background of the Invention

Today, commercial exhibition of digital motion pictures is becoming increasingly widespread. A method for distributing digital motion picture data is described in United States Patent number 5,924,013 titled "Method and apparatus for transmitting motion picture cinematic information for viewing in movie theaters and ordering method therefor," issued to Guido, et al ("Cinematic Information Patent").

Prevention of theft of cinematic intellectual property is an important issue in the commercialization and distribution of electronic, digital cinema. As described in the cinematic information patent cited above, digital cinema requires distribution of movies in the form of digital data. Digital data is vulnerable to quick, inexpensive, and accurate duplication. However, the cinematic information patent cited above, and other prior art in the field of electronic, digital cinema does not provide a mechanism to prevent or hamper the theft of the digital movie data.

One way to secure digital data is encryption. Many encryption techniques and algorithms are known, and can be used to encrypt digital movie data before it is distributed.

Distribution of encrypted movie data requires that a key to decrypt the data be obtained by a theater operator who wishes to exhibit the movie. To maintain a single inventory of movie data by the distribution company, it is desirable to encrypt all copies of a given movie title utilizing a single key. However, it is also desirable to ensure that only an individual, authorized exhibitor be able to decrypt and exhibit an individual distributed copy of a motion picture intended for that exhibitor. Existing encryption technology does not provide a way to encrypt multiple copies of data with a single key, and at the same time to ensure that each individual copy can be decrypted by only an individual intended recipient.

Additionally, while encryption can protect electronic data from theft during distribution, it cannot prevent all forms of piracy. In order to exhibit a movie, the encrypted movie data must first be decrypted. Generally, encrypted data is decrypted on a secure computer system which enacts a decryption algorithm, and which stores a decryption key in memory. In the cinematic projection environment, the security of such computer systems and decryption keys is at risk. If theft of the digital data is possible, then it is equally likely that the computers and memory devices that are required to enact the security process are vulnerable to theft as well. Such a security system is thus vulnerable to theft because it can be stolen and used to exhibit the motion picture at another location and in circumvention of restrictions and constraints normally imposed upon the distribution and exhibition of the motion picture.

Another problem with contemporary digital cinema is ensuring that a motion picture can only be exhibited during an authorized range of dates. With traditional film, the film print is returned to the distribution company after the movie exhibition dates have expired. In this manner, the distribution company maintains control over the whereabouts of the movie, preventing unauthorized exhibition and other forms of theft. With digital, electronic motion picture distribution, the data comprising the movie is normally not returned to the

distributor. Thus, techniques are required for ensuring that the movie data can only be played during a fixed, authorized range of dates.

Even where a legitimate, authorized exhibition of the motion picture occurs, the data still remains vulnerable to theft. Currently movie piracy is commonly accomplished through such analog schemes as direct visual image and audio recording of the movie from within the cinema auditorium itself, and contemporary security mechanisms are incapable of tracing the origin of such theft.

Thus improved techniques for safeguarding electronically distributed digital motion picture data are required to obviate movie piracy and the associated issues described above.

Summary of the Invention

In accordance with the present invention, efficient techniques are provided for ensuring secure distribution, receipt, and exhibition of digital audiovisual data. Encrypted digital movie data is provided by a movie distributor to at least one exhibitor. Because the data is encrypted, the distribution is secure.

All distributed copies of a given movie title can be encrypted with the same key, thereby allowing single inventory of movie data by a distributor. In addition to digital movie data, a movie decryption key and exhibitor authorization data are distributed to each exhibitor. The key and authorization data are distributed separately from the movie data, and are preferably encrypted with a key that is unique to the intended exhibitor recipient. Unlike the movie data itself, the key and authorization data need not be singly inventoried by the distributor and thus do not require that all copies be encrypted with the same key.

The exhibitor authorization data contains information uniquely identifying the exhibitor, as well as valid authorized dates for exhibition of the movie. Thus, each exhibitor

receives unique authorization data for each received digital movie. In a preferred embodiment, the exhibitor identification information in the authorization data includes a unique exhibitor identification code, and a location of the exhibitor generated by a global positioning system. Alternatively, other data such as a projector serial number can be used as all or part of the identification information as desired. The authorization data is compared with local data provided by an exhibitor. In a preferred embodiment, local data comprises date, time, and location information provided by a global positioning system receiver. Only upon match up of the local data with the authorization data can the decryption and subsequent exhibition of the movie data occur.

Thus, theft of the movie data, the decryption key, and the authorization data is not sufficient to decrypt and exhibit the movie, since local data must match the authorization data in order to decrypt and exhibit the movie. Although theft of an exhibitor's computer system and projector remains possible, an attempt to exhibit the movie at another location will fail due to the mismatch between the authorization data and local data that includes global positioning data. Therefore, if a thief attempts an unauthorized exhibition of stolen movie data at another location, the local data will be absent or will not match the authorization data. Even if the thief is in possession of the exhibitor's projection equipment and global positioning system receiver, the location data generated by the global positioning system receiver will not match the location data of the authorized exhibitor.

Additionally, the authorization data contains the range of authorized dates during which the movie may be exhibited, and the local data to be compared with the authorization data includes the date. Thus, the movie cannot be decrypted or exhibited outside of the range of authorized dates.

Before the digital movie data is sent to the projection mechanism and the audio playback system, signature data is presented to a device analogous to a watermarking device

which encodes a unique signature into the visual image and audio signals. This signature is based upon information which uniquely identifies the exhibitor. In a preferred embodiment, the signature data is similar to the authorization data, and can include an exhibitor identification number, date, time, and location. The signature data can be recovered from illicitly copied material. Known methods can be used to create such a so-called watermark that can then be recovered from analog copies of data. Thus, the watermark provides a scheme for identifying the exhibition source of a pirated copy of a movie, even where the theft involves analog copying.

Brief Description of the Drawings

FIG. 1 is a flowchart illustrating the process of distributing digital audiovisual data to at least one exhibitor in accordance with one preferred embodiment of the present invention.

FIG. 2 is a flowchart illustrating the process of receiving and exhibiting digital audiovisual data by an exhibitor in accordance with one preferred embodiment of the present invention.

FIG. 3 is a block diagram illustrating a system utilized to ensure that an exhibitor is authorized to exhibit the digital audiovisual data in accordance with an embodiment of the present invention.

FIG. 4 is a block diagram illustrating exhibitor identification data in accordance with one embodiment of the present invention.

Detailed Description of the Invention

The present invention enables secure distribution, receipt, and exhibition of digital audiovisual data. The term " audiovisual" is used herein to mean "audio" or "visual." The digital audiovisual data is distributed by a distributor to at least one exhibitor. For security of distribution, the digital audiovisual data is encrypted. Each exhibitor securely receives the encrypted digital audiovisual data. The authorization of the exhibitor is verified, and only upon verification is an exhibitor allowed to decrypt and exhibit the digital audiovisual data. Prior to exhibition, the audiovisual data is encoded with unique data identifying the exhibitor. Unauthorized analog copies made from the exhibition of audiovisual data can be traced through the identifying data.

The flowchart of FIG. 1 illustrates the process of distributing digital audiovisual data according to an embodiment of the present invention. A distributor encrypts 101 digital audiovisual data. Preferably, the digital audiovisual data comprises a motion picture, but the digital audiovisual data may also comprise television programs, visual image communication data, and the like, as desired. A known encryption method such as RSA, Skipjack, DES, Blowfish, or the like is utilized to encrypt 101 the digital audiovisual data. Preferably, every copy of a motion picture (or other audiovisual data in alternative embodiments) is encrypted 101 using a single key, to facilitate single inventory of the data by the distributor. In alternative embodiments, each copy of a motion picture may be encrypted with a separate, unique key.

In a preferred embodiment of the present invention, the digital audiovisual data is encrypted in a conventional manner by computer software residing in memory of a computer system including a central processing unit. In alternative embodiments, the digital audiovisual data may be encrypted by hardware, firmware, or any combination of software, hardware and firmware, as desired.

Once the digital audiovisual data is encrypted, the distributor assembles 103 exhibitor authorization data for each exhibitor who is to receive the digital audiovisual data. Exhibitor authorization data is used to verify that an exhibitor is authorized to receive and exhibit the digital audiovisual data, and is thus unique for each exhibitor. FIG. 4 illustrates exhibitor identification data 401 in one embodiment of the present invention. Exhibitor authorization data 401 for each exhibitor comprises exhibitor identification information 403, audiovisual data identification information 405, and valid dates of exhibition 407 of the audiovisual data. In alternative embodiments, the exhibitor authorization data 401 may also contain additional information, for example including distributor identification information. In other alternative embodiments, the exhibitor authorization data 401 may contain less information, for example, with valid dates of exhibition 407 omitted because the exhibitor purchased a license to exhibit the audiovisual data without date restrictions.

Preferably, the exhibitor identification information 403 contained in the exhibitor authorization data 401 comprises location information of the exhibitor such as is generated by a global positioning system, and constitutes an authorized location for the exhibition of the digital audiovisual data. Alternatively, exhibitor identification information 403 may comprise other data such as a serial number of an exhibitor's digital movie projector or an assigned exhibitor identification code, as desired.

Preferably, the exhibitor authorization data 401 may also be encrypted 105, or may be present in clear digitized text. In a preferred embodiment, the exhibitor authorization data 401 for each exhibitor is encrypted 105 utilizing a key unique to that exhibitor. Preferably, exhibitor authorization data 401 is distributed to a given exhibitor in encrypted form utilizing that exhibitor's public key of an encryption method such as RSA that requires a public key and a private key. A public and a private key for each exhibitor are preferably generated by the distributor. The public key is used to encrypt 105 exhibitor authorization

data 401, and the private key is used, by the exhibitor, to decrypt the exhibitor authorization data 401. Various secure channels may be utilized to distribute the private key to the exhibitor. Distribution of the private key is discussed in detail later in this specification.

It should be noted that the above-described encryption of the exhibitor authorization data 401 may be modified in alternative embodiments to include public and private keys generated by each exhibitor rather than by the distributor, may be modified to include a single key to encrypt and decrypt the data, and may be modified to include a key that is not unique to the exhibitor. Alternatively, the exhibitor authorization data 401 is not encrypted at all, but instead may appear in clear digitized text, as desired.

In a preferred embodiment, the key to decrypt the encrypted audiovisual data for each exhibitor is encrypted 107 utilizing a key unique to that exhibitor. Preferably, this is the same key used to encrypt 105 the exhibitor authorization data 401, as described above. The alternative embodiments described above for the encryption of the exhibitor authorization data 401 also apply to the encryption of the key to decrypt the audiovisual data.

Next, the digital audiovisual data, the key to decrypt the encrypted audiovisual data, and the exhibitor authorization data 401 are distributed to at least one exhibitor. Preferably, the digital audiovisual data is distributed 109 separately from the key to decrypt the digital audiovisual data, and from the exhibitor authorization data 401, over a secure communication channel, such as telephone, Internet, leased communication line, and the like. The distribution of the digital audiovisual data can be by transmission over such public channels as the Internet, telephone lines, fiber optic cable, satellite, or the like, as desired. Alternatively, the digital audiovisual data may be distributed on magnetic or optical media.

In one preferred embodiment of the present invention, the exhibitor authorization data 401 and the key to decrypt the encrypted audiovisual data are embedded 111 in a computer program to be distributed to an exhibitor. The computer program also contains program code to verify that an exhibitor is authorized to exhibit the audiovisual data, and program code to process the results of the verification. The operation of such computer program is described in detail later in this specification. For each exhibitor to receive the digital audiovisual data, a copy of the computer program is created containing the exhibitor authorization data 401 for that exhibitor, as well as the key to decrypt the digital audiovisual data.

Next, the appropriate copy of the computer program is distributed 113 by conventional schemes to each exhibitor that receives the digital audiovisual data. As with the digital audiovisual data, the computer program is preferably distributed over a secure public channel such as the Internet, but can also be distributed on magnetic or optical media, as desired.

In a preferred embodiment of the present invention, assembling the exhibitor authorization data 401, encrypting the exhibitor authorization data 401, encrypting the key to decrypt the digital audiovisual data, and embedding the exhibitor authorization data 401 and the key to decrypt the encrypted audiovisual data in a copy of the computer program are performed by computer software residing in computer memory of a computer system with a central processing unit. In alternative embodiments, assembling the exhibitor authorization data 401, encrypting the exhibitor authorization data 401, encrypting the key to decrypt the digital audiovisual data, and embedding the exhibitor authorization data 401 and the key to decrypt the encrypted audiovisual data in a copy of the computer program are performed by hardware, firmware, or any combination of software, hardware, and firmware as desired.

FIG. 2 is a flowchart illustrating the steps involved in receiving and exhibiting digital audiovisual data by an exhibitor in accordance with one embodiment of the present invention. In FIG. 2, an exhibitor receives 201 encrypted digital audiovisual data. Typically, the digital audiovisual data comprises a motion picture, but may also be other forms of digitized data as previously explained. Next, the exhibitor receives 203 exhibitor authorization data 401 and a key to decrypt the encrypted audiovisual data. In one preferred embodiment, the receipt of the digital audiovisual data is separate from the receipt of the exhibitor authorization data 401 and from the key to decrypt the encrypted audiovisual data. Preferably, the exhibitor authorization data 401 and key to decrypt the encrypted audiovisual data are embedded in a computer program which is received 203 from the distributor.

Prior to decrypting the digital audiovisual data and allowing exhibition thereof, the exhibitor must be verified to have present authorization to exhibit the digital audiovisual data. FIG. 3 illustrates one system utilized for verification of this authorization and subsequent exhibition of digital audiovisual data in accordance with one embodiment of the present invention. A computer system 301 contains a central processing unit 303, computer memory 305, and storage device 307 such as at least one magnetic disk or at least one writeable optical disk. Data is received via at least one input mechanism 309 such as modem, cable, network card, satellite receiver, floppy disk drive, and the like, and is transmitted to audiovisual data exhibition hardware via an output mechanism 311. In one preferred embodiment, the audiovisual data exhibition hardware comprises a digital projector 313 and an audio playback system 315. The computer system 301, digital projector 313 and audio playback system 315 can all be components of a single physical device, or can be separate, physically discrete devices as desired. Separate hardware components of these types are required to be physically or logically connected, for example

by a local area computer network, by telephone lines, or by a wireless, electromagnetic radiation-based communication system. In one embodiment, the computer system 301 is a component of the digital projector 313.

Referring again to FIG. 2 and FIG. 3, the computer program 317 is loaded into the computer memory 305 of the computer system 301 via an input mechanism 309. The computer program 317 is then executed 205 by the central processing unit 303 of the computer system 301 to retrieve 207 exhibitor identification data 319 that uniquely identifies the exhibitor. Preferably, the exhibitor identification data 319 comprises a location of the exhibitor and a current date. This information is preferably provided by a global positioning system (GPS) receiver 321 coupled to the computer system 301. Alternatively, the exhibitor identification data 319 comprises other information such as a digital projector serial number or an assigned exhibitor identification code, as desired.

Next, the computer program 317 verifies that the exhibitor is authorized to exhibit the digital audiovisual data 327 at a current date within a range of dates. Where the exhibitor authorization data 401 is encrypted, as in one preferred embodiment, the computer program 317 must decrypt 209 it in order to proceed. To do so, the computer program 317 preferably accesses the private key 325 of the exhibitor. As explained above, the private key 325 is preferably unique to the exhibitor, and is supplied by the distributor. In a preferred embodiment of the present invention, the private key 325 is distributed to the exhibitor on physical media, such a floppy disk or CD-ROM. Alternatively, the private key 325 can be distributed over a secure transmission channel such as the Internet, or the like, as desired. In one embodiment, the private key 325 is stored by the distributor, and accessed by the exhibitor as needed. In such an embodiment, the identification of the exhibitor is verified prior to allowing access of the private key 325. In every embodiment that includes a private key 325, a new private key 325 is generated from time to time and made available

to the exhibitor. In an alternative embodiment, the public and private key combination is generated by the exhibitor instead of by the distributor. In that embodiment, the public key is made available to the distributor and used for the encryption. The private key 325, held by the exhibitor, is then used for the decryption.

Once the exhibitor authorization data 401 has been decrypted 209, the computer program 317 proceeds to verify that the exhibitor is authorized to exhibit the digital audiovisual data 327. To do so the computer program 317 first compares 211 the exhibitor authorization data 401 to the exhibitor identification data 319. Preferably an authorized location for the exhibition of the digital audiovisual data 327 in the exhibitor authorization data 401 provided by the distributor is compared 211 with the location of the exhibitor contained in the exhibitor identification data 319. As explained above, the location of the exhibitor contained in the exhibitor identification data 319 is preferably provided by a GPS receiver 321. Because the location of the authorized exhibitor is known to the distributor and is included in the exhibitor authorization data 323, the location of the exhibitor provided by the GPS receiver 321 can be used to verify the authorization of the exhibitor. Even if the digital audiovisual data 327, projection equipment 313, and GPS receiver 321 are stolen, the digital audiovisual data 327 will still be secure. The authorization check performed prior to exhibition will fail at least because the stolen and relocated GPS receiver 321 will report a different location from that provided by the distributor. The comparison of GPS location data is performed with moderate precision and not finite precision, so that movement of the GPS receiver 321 or antenna within an exhibitor's site does not result in a verification failure. In alternative embodiments, data other than location is used to verify the identity of the exhibitor such as a serial number of the projection equipment 313, or a password, or the like.

Once the identity of the exhibitor has been confirmed, the current date is verified 213 against the range of dates during which the exhibitor is authorized to exhibit the digital audiovisual data 327. As explained above, this range of dates is preferably included in the exhibitor authorization data 323. The current date is preferably provided by the GPS receiver 321. Alternatively, the current date is provided by the operating system of the computer system 301. Either way, the computer program 307 verifies 213 that the current date is within the authorized range.

If the identity of the exhibitor and the date are successfully verified, the exhibition of the digital audiovisual data 327 is allowed to proceed. However, if either the identity of the exhibitor, or the authorization to exhibit on the current date is not confirmed, the computer program 317 does not decrypt the digital audiovisual data 327, which therefore cannot be exhibited 215. Preferably, the computer program 317 erases the digital audiovisual data 327 and decryption key. Preferably the computer program 317 transmits a control signal to the distributor indicating that an attempt is occurring to execute an unauthorized exhibition of the digital audiovisual data 327 at a given location. Then, the computer program 317 terminates.

If the identity of the exhibitor and the date are successfully verified, the computer program 317 proceeds to decrypt 217 the key 325 needed to decrypt the digital audiovisual data 327. This key 325 is preferably encrypted with the same key as the exhibitor authorization data, and is decrypted in the same manner, as described above. Once the key 325 to decrypt the digital audiovisual has been decrypted, the digital audiovisual data 327 is then decrypted 219 by the computer program 317. At this point, the audiovisual data is ready to be watermarked prior to exhibition.

The use of the computer program 317 as described above represents one mode of practicing the present invention, in alternative embodiments of the present invention, there

is no computer program 317, and the exhibitor authorization data 401 and key 325 to decrypt the digital audiovisual data 327 are received by themselves. In such embodiments, the exhibitor authorization data 401 and key 325 to decrypt the digital audiovisual data 327 are loaded into the computer memory 305 of the computer system 301 at the exhibitor site. Then, all of the steps that are performed by the computer program 317 in the embodiment described above are instead performed by software (or, in other embodiments by hardware, firmware, or any combination of software, hardware, and firmware as desired) which comprises a component of the exhibitor's computer system 301.

To enable tracking of theft in the form of analog copying of the exhibition of the audiovisual data, the audiovisual data is watermarked 221 with unique identifying data prior to exhibition. The identifying data can be provided by a date and time clock, or a memory device containing unique data stored by the projector manufacturer, or a memory device containing unique data stored by the exhibitor, or unique signature data provided through a local-area network (LAN), or the GPS receiver 321. Preferably the identifying data comprises the location and date information provided by the GPS receiver 321.

The present invention is not dependent upon the choice of watermarking technology used to encode the identifying information in the visual image and audio signal. Various known watermarking technologies that are currently commercially available can be utilized as desired to watermark 221 both visual image and audio signals, or alternatively to watermark 221 only the audio signal or only the visual image signal. Watermarking technology, by its nature, imprints the data with the watermarking information which can facilitate the recovery of the encoded identifying data, and thus aid in the identification of an analog theft. Once the data is watermarked 221, it can be exhibited 223.

What is claimed is:

1. A method for ensuring secure receipt and secure, authorized exhibition of digital audiovisual data by an exhibitor, the method comprising:

receiving encrypted digital audiovisual data;

receiving exhibitor authorization data that uniquely identifies the exhibitor;

receiving a key to decrypt encrypted digital audiovisual data;

retrieving exhibitor identification data that uniquely identifies the exhibitor;

verifying that the exhibitor is authorized to exhibit the digital audiovisual data by comparing the received exhibitor authorization data to the retrieved exhibitor identification data;

only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, decrypting the encrypted digital audiovisual data; and

only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, allowing exhibition of the audiovisual data by the exhibitor.

2. The method of claim 1 wherein the received key to decrypt the digital audiovisual data is itself encrypted and the method further comprises:

decrypting the received key to decrypt the digital audiovisual data.

3. The method of claim 2 further comprising:

decrypting the received key to decrypt the digital audiovisual data with a key unique to the exhibitor.

4. The method of claim 1 wherein the received exhibitor authorization data is encrypted and the method further comprises:

decrypting the received exhibitor authorization data.

5. The method of claim 4 further comprising:

decrypting the received exhibitor authorization data with a key unique to the exhibitor.

6. The method of claim 1 wherein the received exhibitor authorization data includes a range of dates during which the exhibitor is authorized to exhibit the digital audiovisual data, and the method further comprises:

comparing a current date to the range of authorized exhibition dates in the received exhibitor authorization data;

only in response to the current date being within the range of authorized exhibition dates, decrypting the digital audiovisual data; and

only in response to the current date being within the range of authorized exhibition dates, allowing exhibition of the audiovisual data by the exhibitor.

7. The method of claim 1 wherein the received exhibitor authorization data includes a location at which the exhibitor is authorized to exhibit the digital audiovisual data, and the method further comprises:

comparing a current location to the location for authorized exhibition in the received exhibitor authorization data;

only in response to the current location being the authorized exhibition location, decrypting the digital audiovisual data; and

only in response to the current location being the authorized exhibition location, allowing exhibition of the digital audiovisual data by the exhibitor.

8. The method of claim 7 wherein the current location is provided by a global positioning system receiver.

9. The method of claim 1 wherein the exhibitor authorization data and the key to decrypt the digital audiovisual data are embedded in a computer program, and the method further comprises:

receiving the computer program in which the exhibitor authorization data and the key to decrypt the digital audiovisual data are embedded;

executing the computer program; and

verifying, by the computer program, that the exhibitor is authorized to exhibit the digital audiovisual data by comparing the received exhibitor authorization data to the retrieved exhibitor identification data.

10. The method of claim 9 further comprising:

in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, decrypting, by the computer program, the encrypted digital audiovisual data.

11. The method of claim 9 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, prohibiting decryption of the encrypted digital audiovisual data by the computer program.

12. The method of claim 9 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, prohibiting exhibition of audiovisual data by the computer program.

13. The method of claim 12 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, deleting the digital audiovisual data by the computer program.

14. The method of claim 9 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, transmitting to the distributor, by the computer program, a control signal indicating that an unauthorized exhibition is being attempted.

15. The method of claim 1 further comprising:

prior to exhibiting the digital audiovisual data, including identifying data within the audiovisual data, the identifying data uniquely identifying the exhibitor.

16. The method of claim 15 wherein the identifying data is included only within the visual image portion of the data.

17. The method of claim 15 wherein the identifying data is included only within the audio portion of the data.

18. The method of claim 1 wherein the receipt of the encrypted digital audiovisual data is separate from the receipt of the exhibitor authorization data and from the key to decrypt the encrypted digital audiovisual data.

19. The method of claim 1 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, prohibiting exhibition of audiovisual data.

20. The method of claim 19 further comprising:

in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, deleting the digital audiovisual data.

21. A method for securely distributing digital audiovisual data to at least one exhibitor, ensuring only authorized exhibition of the digital audiovisual data, the method comprising:

encrypting digital audiovisual data;

distributing the encrypted digital audiovisual data to at least one exhibitor;

distributing a key to decrypt the encrypted digital audiovisual data to at least one exhibitor;

for each exhibitor to receive the audiovisual data, assembling exhibitor authorization data unique to that exhibitor; and

distributing exhibitor authorization data to at least one exhibitor.

22. The method of claim 21 further comprising:

embedding the decryption key and the exhibitor authorization data in a computer program;

including in the computer program code for verifying that an exhibitor is authorized to exhibit the digital audiovisual data; and

distributing the computer program to at least one exhibitor.

23. The method of claim of 21 wherein the exhibitor authorization data includes an authorized location for the exhibition of the digital audiovisual data.

24. The method of claim of 21 wherein the digital audiovisual data is encrypted using a single key and distributed to at least two exhibitors.

25. The method of claim of 21 further comprising:

prior to distributing the key to decrypt the encrypted digital audiovisual data, for each exhibitor to receive the audiovisual data, encrypting the key to decrypt the encrypted digital audiovisual data with a key unique to that exhibitor.

26. The method of claim of 21 further comprising:

prior to distributing exhibitor authorization data, for each exhibitor to receive the audiovisual data, encrypting the exhibitor authorization data with a key unique to that exhibitor.

27. The method of claim of 21 wherein the distribution of the encrypted digital audiovisual data is separate from the distribution of the key to decrypt the encrypted digital audiovisual data and from the exhibitor authorization data.

28. A computer program product on a computer readable medium for ensuring secure receipt and secure, authorized exhibition of digital audiovisual data by an exhibitor, the computer program product comprising:

program code for receiving encrypted digital audiovisual data;

program code for receiving exhibitor authorization data that uniquely identifies the exhibitor;

program code for receiving a key to decrypt encrypted digital audiovisual data;

program code for retrieving exhibitor identification data that uniquely identifies the exhibitor;

program code for verifying that the exhibitor is authorized to exhibit the digital audiovisual data by comparing the received exhibitor authorization data to the retrieved exhibitor identification data;

program code for, only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, decrypting the encrypted digital audiovisual data; and

program code for, only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, allowing exhibition of the audiovisual data by the exhibitor.

29. The computer program product of claim 28 wherein the received exhibitor authorization data includes a range of dates during which the exhibitor is authorized to exhibit the digital audiovisual data, and the computer program product further comprises:

program code for comparing a current date to the range of authorized exhibition dates in the received exhibitor authorization data;

program code for, only in response to the current date being within the range of authorized exhibition dates, decrypting the digital audiovisual data; and

program code for, only in response to the current date being within the range of authorized exhibition dates, allowing exhibition of the audiovisual data by the exhibitor.

30. The computer program product of claim 28 wherein the received exhibitor authorization data includes a location at which the exhibitor is authorized to exhibit the digital audiovisual data, and the computer program product further comprises:

program code for comparing a current location to the location for authorized exhibition in the received exhibitor authorization data;

program code for, only in response to the current location being the authorized exhibition location, decrypting the digital audiovisual data; and

program code for, only in response to the current location being the authorized exhibition location, allowing exhibition of the digital audiovisual data by the exhibitor.

31. The computer program product of claim 28 further comprising:

program code for, prior to exhibiting the digital audiovisual data, including identifying data within the audiovisual data, the identifying data uniquely identifying the exhibitor.

32. The computer program product of claim 31 further comprising program code for including identifying data only within the visual image portion of the data.

33. The computer program product of claim 31 further comprising program code for including identifying data only within the audio portion of the data.

34. The computer program product of claim 28 further comprising:

program code for, in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, prohibiting exhibition of audiovisual data.

35. The computer program product of claim 34 further comprising:

program code for, in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, deleting the digital audiovisual data.

36. The computer program product of claim 28 further comprising:

program code for, in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, prohibiting decryption of the encrypted digital audiovisual data by the computer program.

37. The computer program product of claim 28 further comprising:

program code for, in response to failure of verification of the exhibitor's authorization to exhibit the digital audiovisual data, transmitting to the distributor, by the computer program, a control signal indicating that an unauthorized exhibition is being attempted.

38. A computer program product on a computer readable medium for securely distributing digital audiovisual data to at least one exhibitor, ensuring only authorized exhibition of the digital audiovisual data, the computer program product comprising:

program code for encrypting digital audiovisual data;

program code for distributing the encrypted digital audiovisual data to at least one exhibitor;

program code for distributing a key to decrypt the encrypted digital audiovisual data to at least one exhibitor;

program code for assembling, for each exhibitor to receive the audiovisual data, exhibitor authorization data unique to that exhibitor; and

program code for distributing exhibitor authorization data to at least one exhibitor.

39. A method for securely distributing and receiving digital audiovisual data, ensuring only authorized exhibition of the digital audiovisual data, the method comprising:

encrypting digital audiovisual data;

distributing the encrypted digital audiovisual data to at least one exhibitor;

distributing a key to decrypt the encrypted digital audiovisual data to at least one exhibitor;

for each exhibitor to receive the audiovisual data, assembling exhibitor authorization data unique to that exhibitor;

distributing exhibitor authorization data to at least one exhibitor;

receiving encrypted digital audiovisual data by at least one exhibitor;

receiving unique exhibitor authorization data by at least one exhibitor;

receiving a key to decrypt encrypted digital audiovisual data by at least one exhibitor;

retrieving unique exhibitor identification data;

verifying that the exhibitor is authorized to exhibit the digital audiovisual data by comparing the received exhibitor authorization data to the retrieved exhibitor identification data;

only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, decrypting the encrypted digital audiovisual data; and

only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, allowing exhibition of the audiovisual data by the exhibitor.

40. An apparatus for ensuring secure receipt and secure, authorized exhibition of digital audiovisual data by an exhibitor, the apparatus comprising:

a computer system having a central processing unit, memory, at least one input, at least one output, and storage, for processing input and output, and for ensuring secure receipt and exhibition of digital audiovisual data;

in the memory of the computer system, a reception module, for receiving encrypted digital audiovisual data, for receiving unique exhibitor

authorization data, and for receiving a key to decrypt the encrypted digital audiovisual data;

in the memory of the computer system, a retrieval module, for retrieving unique exhibitor identification data;

in the memory of the computer system and coupled to the reception module and to the retrieval module, a verification and comparison module, for verifying that the exhibitor is authorized to exhibit the digital audiovisual data by comparing the received exhibitor authorization data to the retrieved exhibitor identification data;

in the memory of the computer system and coupled to the verification and comparison module, a decryption module for, only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, decrypting the encrypted digital audiovisual data; and

coupled to the computer system, a visual image exhibition module, for exhibiting an visual image portion of audiovisual data;

coupled to the computer system, an audio playback module, for playing back an audio portion of audiovisual data; and

in the memory of the computer system and coupled to the verification and comparison module, an output module for, only in response to verification of the exhibitor's authorization to exhibit the digital audiovisual data, outputting the audiovisual data to the visual image exhibition module and to the audio playback module.

41. The apparatus of claim 40 further comprising:

a global positioning system receiver, coupled to the retrieval module, for providing current location data as exhibitor identification information.

42. The apparatus of claim 40 further comprising:

a watermarking module, coupled to the computer system, for embedding data uniquely identifying the exhibitor within the audiovisual data.

43. A memory for storing data for access by an application program being executed on a computer system, the memory containing:

exhibitor identification information uniquely identifying an individual exhibitor;

digital audiovisual data identification information uniquely identifying specific digital audiovisual data; and

a range of dates during which the individual exhibitor is authorized to exhibit the audiovisual data.

44. The memory of claim 43 wherein the exhibitor identification information comprises location information of the individual exhibitor.

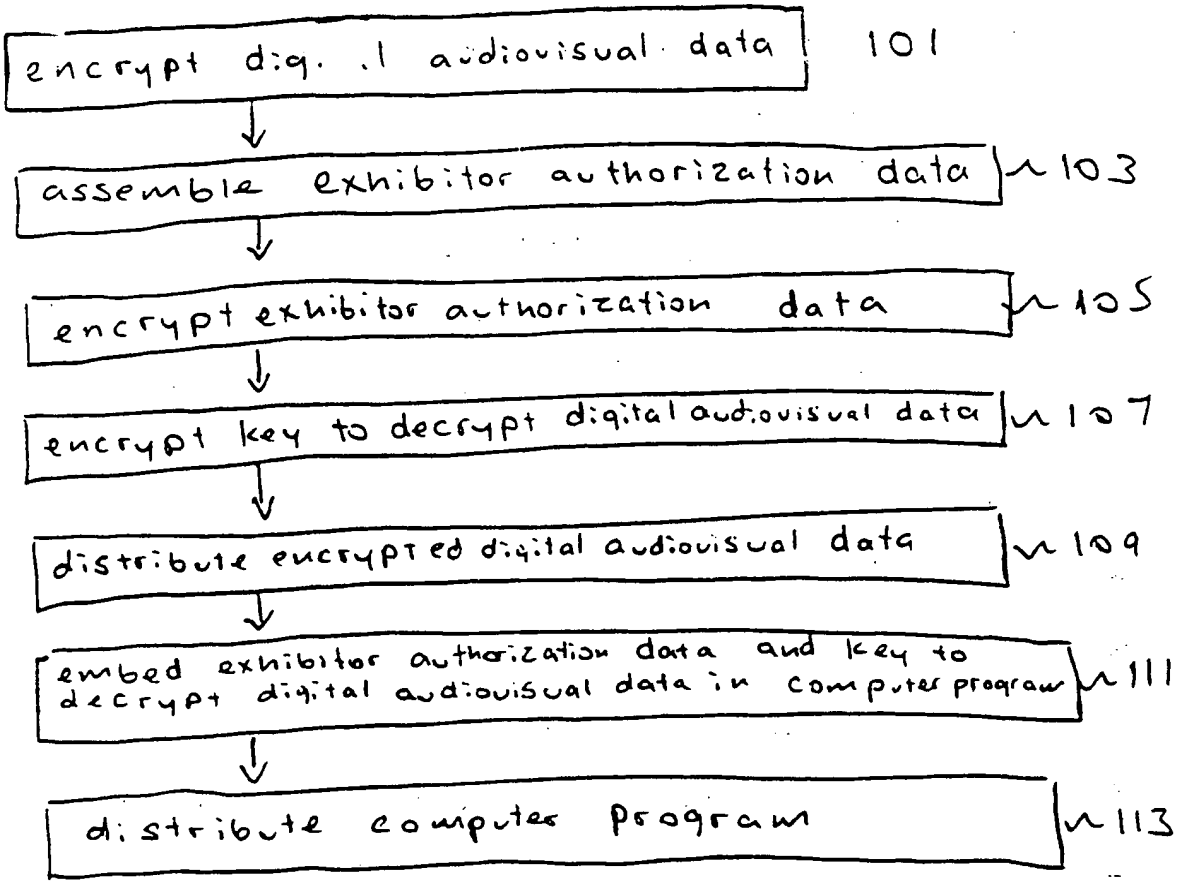

encrypt dig. .l audiovisual data
101
assemble exhibitor authorization data
103
encrypt exhibitor authorization data
105
encrypt key to decrypt digital audiovisual data
107
distribute encrypted digital audiovisual data
109
embed exhibitor authorization data and key to decrypt digital audiovisual data in computer program
111
distribute computer program
113

FIG. 1

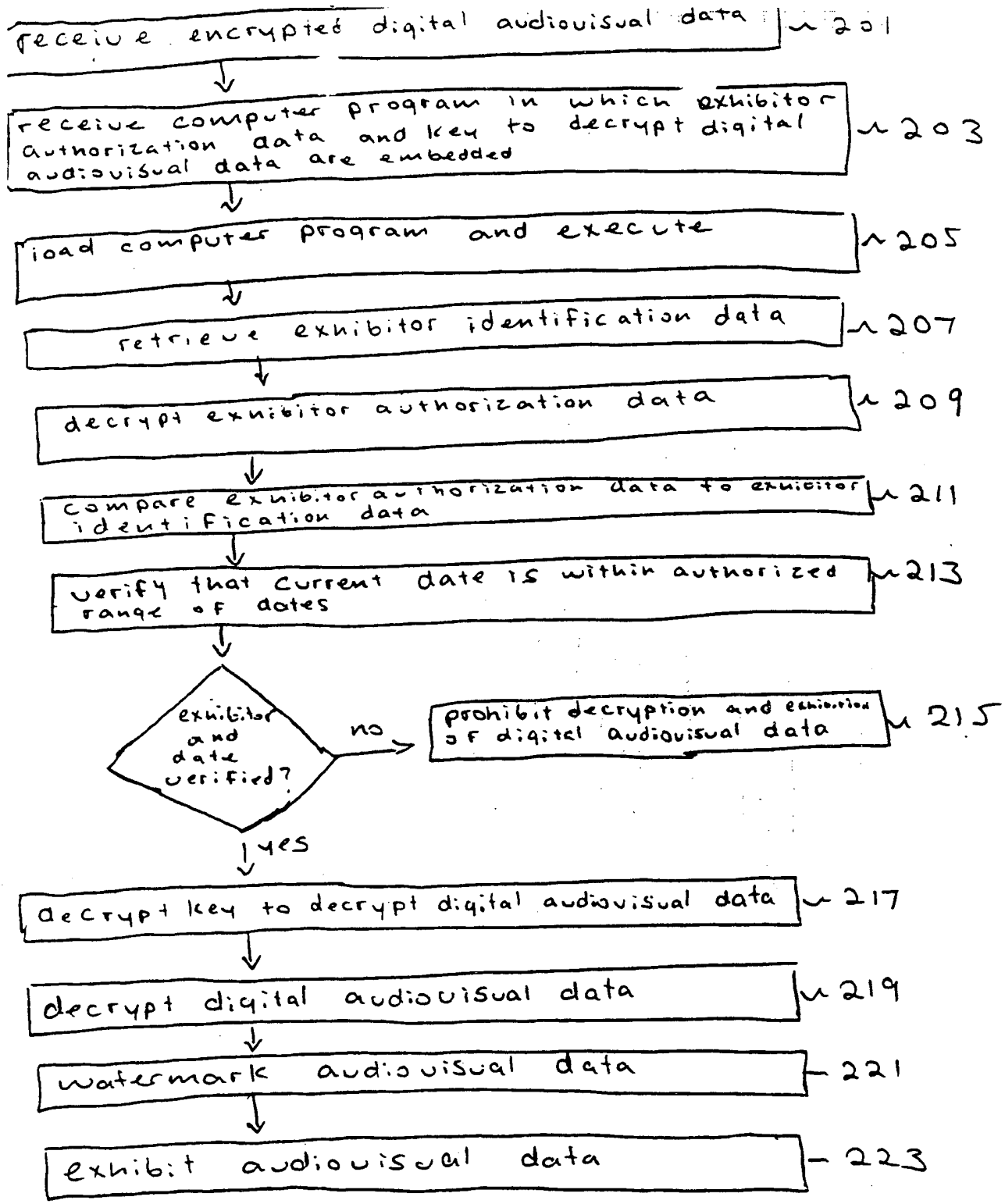

receive encrypted digital audiovisual data
201
receive computer program in which exhibitor authorization data and key to decrypt digital audiovisual data are embedded
203
load computer program and execute
205
retrieve exhibitor identification data
207
decrypt exhibitor authorization data
209
compare exhibitor authorization data to exhibitor identification data
211
verify that current date is within authorized range of dates
213
exhibitor and date verified?
no
prohibit decryption and exhibition of digital audiovisual data
215
yes
decrypt key to decrypt digital audiovisual data
217
decrypt digital audiovisual data
219
watermark audiovisual data
221
exhibit audiovisual data
223

FIG. 2

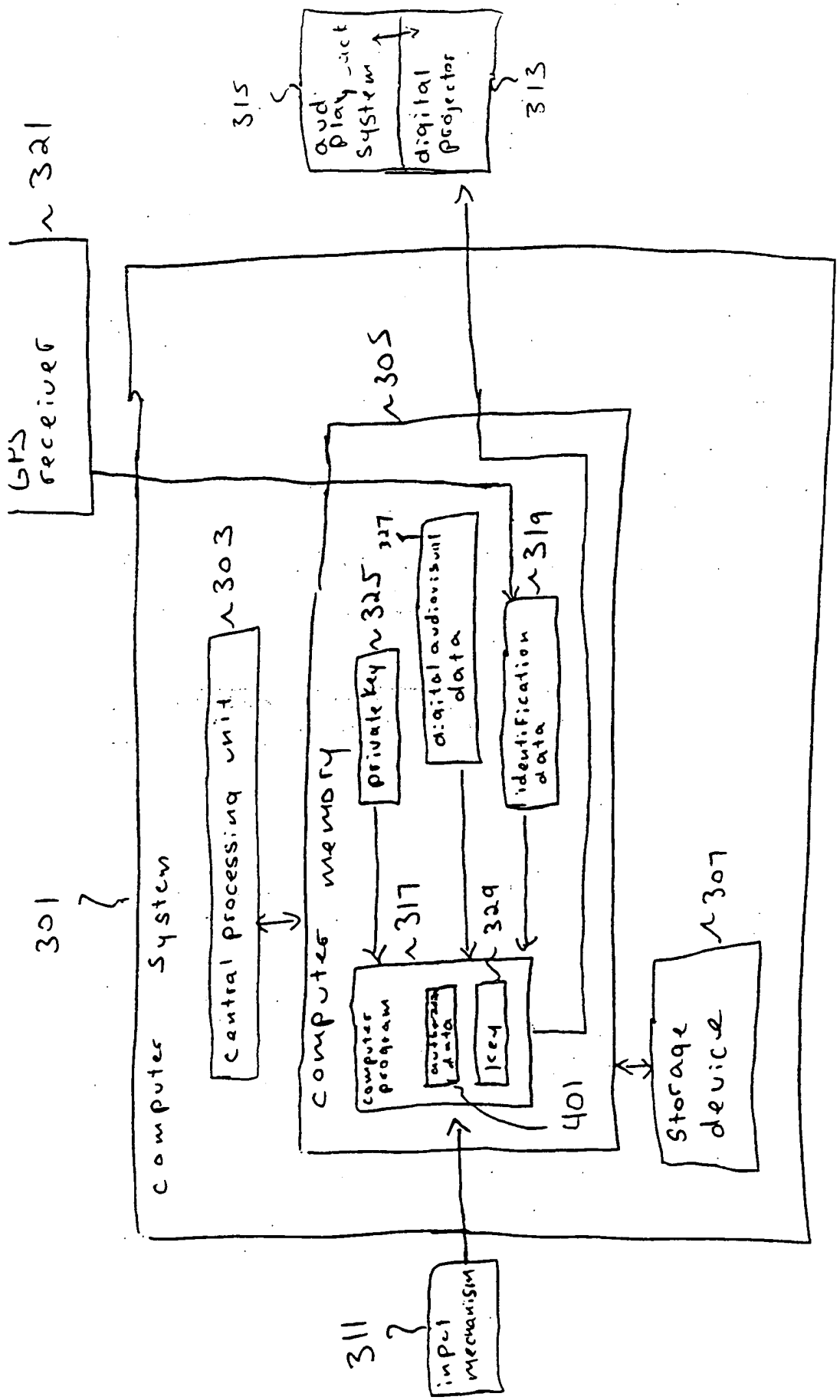

315
audio playback system
digital projector
313
321
GPS receiver
305
303
central processing unit
computer memory
325
private key
327
digital audiovisual data
319
identification data
301
computer system
317
329
computer program
authorization data
key
401
storage device
307
311
input mechanism

FIG. 3

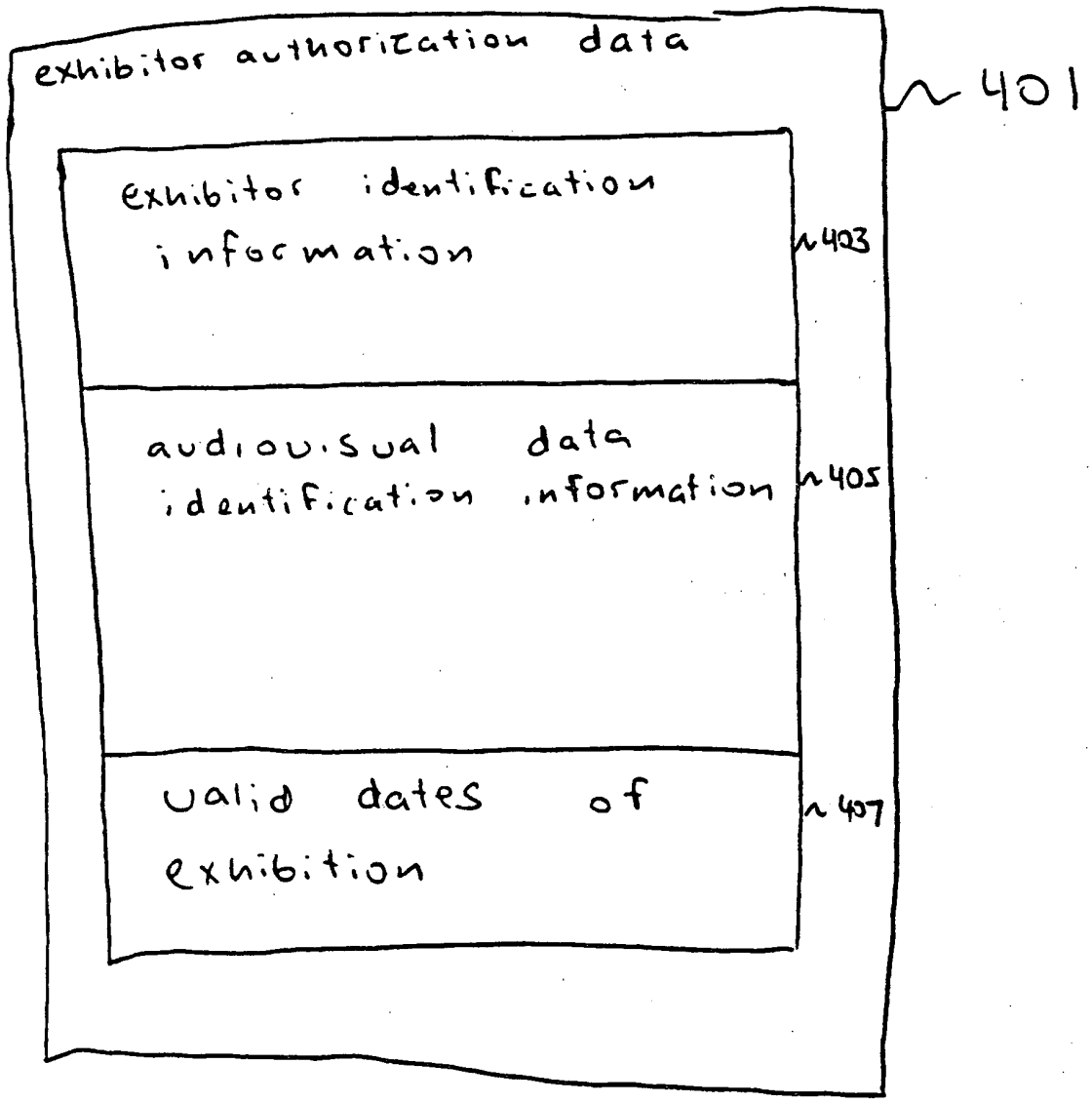

exhibitor authorization data
401
exhibitor identification information
403
audiovisual data identification information
405
valid dates of exhibition
407

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41520

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04N 7/167
US CL : 380/201,202,203,241

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/201,202,203,241

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,751,732 A(KAMITAKE) 14 JUNE 1988, col.5, lines 21-24, col.6, lines 25-30, col.11, lines 20-27,52-60	1-44
Y	US 4,739,510 A(JEFFERS et al) 19 April 1988, col.4, lines 32-36, col.22, lines 11-23	1-44
A	US 5,142,576 A(NADAN) 25 August 1992, col.2, lines 16-26, col.3, lines 13-22, 41-45	1-44

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 09 FEBRUARY 2001	Date of mailing of the international search report 23 MAR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-0040	Authorized officer GILBERTO BARRON James R. Matthews Telephone No. (703) 305-1830

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41520

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

EAST, STN
search terms: encrypt, cipher,encipher,transmit,
send,receive,data,software,program,signal,video,authorize,permission,view,display,key,ID,compare,match